Federal Computer Incident Response Center

The FedCIRC Bits & Bytes

A monthly newsletter for Information System Security Managers/Officers & System Administrators

August 1, 2001 Volume II, Issue 6

TechNotes

Social Engineering

"Social engineering" is the process of exploiting human nature to obtain protected information on a company's infrastructure, policies, procedures, user information and passwords. The process is all too often successful and typically results in unauthorized and undetected access to networks and sensitive information. Hackers and virus writers frequently employ social engineering practices to increase the success of their hostile efforts.

A would-be perpetrator might visit a company web site extracting information on the organization's structure, names and contact information for support or management personnel. By using the freely available contact information, he or she simply calls the individual, posing as someone from the organization's help desk, talks about troubleshooting of a fictitious network problem or validation of the network user information and deceives the individual into surrendering their userID and/or password. Once in possession of that information, the perpetrator may use it to gain access to the network at any time. The network privileges of the legitimate user are now in the hands of the perpetrator. Alternatively, the perpetrator, armed only with an individuals name, may call the help desk posing as the legitimate user and indicate that he/she has forgotten their password. Typically, the help desk will reset the account to a default password, provide the password to the caller and instruct them to change it with their first login. The perpetrator now controls the user's account. The legitimate user can no longer gain the required access and any and all information previously available to the employee is free for the taking. If strict procedures to thwart social engineering practices are not in place, periodically reviewed and tested, then your network and its information are potential targets for exploitation.

As more and more organizations allow remote access to their network enclaves, the complexities associated with protecting network resources increases exponentially. Only a small percentage of home computer users understand the necessity of securing their systems. With the explosive growth of the Internet, the home user is faced with, and too often confused about, the countless threats hiding in cyberspace. The network to which they may connect assumes any insecurity in the home user's system. Remote access should follow a stringent set of security standards. Each home Internet user's system should be afforded a level of protection consistent with that of the parent network and inspected to validate the protection profile prior to allowing the remote connection. Social engineering efforts targeting remote users take new form by allowing the hacker to obtain a user's information from web sites, email and other publicly available sources. Then, posing as the user's Internet service provider, the intruder initiates a call to the user and, under the guise of "verifying user information," deceives the victim into verifying their contact and login information and possibly associated billing information including address and credit card data. Armed with that information, the perpetrator may assume the identity of the victim and cause immeasurable personal and financial damage.

Social engineering is seen in everyday Internet information exchanges. Bogus email is often a medium through which malicious code (viruses, worms, trojans, etc.) is propagated. A recent example was the "Anna Kournikova" worm. This worm exploited

human curiosity and enticed users to open a file that they received via the Internet, unleashing the worm on other unsuspecting victims.

To combat social engineering, users must be educated and apply common sense when reading their e-mail and associated attachments. Certain file extensions such as ".exe, .dll, .doc, .ppt, .xls and .pif" tell us that the file does or may contain executable code. Microsoft Windows®, as a default, hides selected files names. When this option is active, the user may not be able to identify the file as harboring the executable code. Since executable code may be malicious in nature, the option to hide file extensions should always be disabled. Periodic user awareness training should emphasize these issues. Organizations must train users to a level that prepares them to securely function in cyberspace. The cost of effective user training is small compared to the cost of damage control and recovery.

Calendar of Events

Information Security for Technical Staff
Date: August 20-24, 2001
Location: Pittsburgh, PA
POC: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC)
412-268-7702
http://www.cert.org/nav/training.html#infosecurity

Managing Risks to Information Assets
Date: August 20-24, 2001
Location: Pittsburgh, PA
POC: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC)
412-268-7702
http://www.cert.org/nav/training.html#infosecurity

Overview of Creating a Computer Security Incident Response Team
Date: August 30, 2001
Location: Pittsburgh, PA
POC: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC)
412-268-7702
http://www.cert.org/nav/training.html#infosecurity

InfoWarCon 2001: Techniques & Strategies for Securing Shared Infrastructures
Date: September 4-7, 2001
Location: Washington, DC
POC: MIS Training Institute
508-879-7999
http://www.misti.com/conference_show.asp

IO Wargames
Date: September 16-21, 2001
Location: Washington, DC
POC: Sans Institute
540-372-7066
http://www.incidents.org/IOwargames/index.htm

Latest FedCIRC Advisories

FedCIRC Advisory FA-2001-23
Continued Threat of the "Code Red" Worm

FedCIRC Advisory FA-2001-22
W32/Sircam Malicious Code

FedCIRC Advisory FA-2001-21
Buffer Overflow in telnetd

FedCIRC Advisory FA-2001-20
Continuing Threats to Home Users

FedCIRC Advisory FA-2001-19
"Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL

FedCIRC Advisory FA-2001-18
Multiple Vulnerabilities in Several Implementations of the Ligthweight Directory Access Protocol (LDAP)

FedCIRC Advisory FA-2001-17
Check Point RDP Bypass Vulnerability

FedCIRC Advisory FA-2001-16
Oracle 8i Contains Buffer Overflow in TNS Listener

The FedCIRC Bits & Bytes Newsletter

Technical Director
David Jarrell
Liaison Director
Lawrence Hale
Operations Liaison
Connie Oden
Editor
Corliss A. McCain
Contributing Editors
David Adler
Kenneth Grossman
Michael C. Smith

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions is the 15th of each month. Articles may be edited for length and content. Back issues of this newsletter can be found on the FedCIRC website www.fedcirc.gov/docs.html

FedCIRC is sponsored by the Federal CIO Council and is operated by the General Services Administration/Federal Technology Service